пам'ятка клієнта

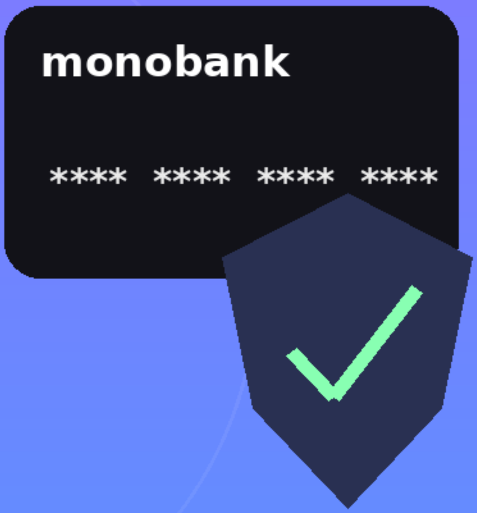
Безпека в mono

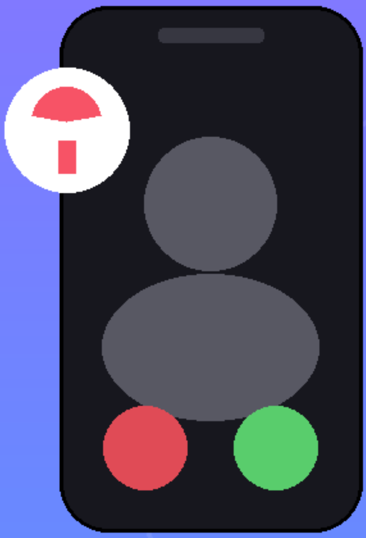
Пам'ятка для клієнтів: як розпізнати шахраїв, не передати дані й правильно діяти, якщо вам дзвонять або пишуть від імені банку.

Якщо шукаєте інформацію про **Монобанк**,
відкривайте лише перевірені матеріали або застосунок mono.

Головне правило

Якщо розмова змушує поспішати, встановити програму, назвати код або переказати гроші - зупиніться. Це найчастіше ознака шахрайства.





пам'ятка клієнта

Якщо вам телефонують

Перше питання не «що сталося?», а «чи є підтвердження в застосунку?». Справжній контакт mono має перевірятися через monobank, а не через слова людини в телефоні.

Не робіть під час дзвінка

- не називайте SMS-коди, PIN, CVV/CVC або паролі
- не встановлюйте застосунки за інструкцією незнайомця
- не переказуйте кошти на «безпечний» рахунок

Правильна дія

Завершіть розмову. Відкрийте застосунок mono і перевірте повідомлення. Якщо підтвердження немає - не продовжуйте контакт.

пам'ятка клієнта

Якщо вам пишуть

Шахраї часто починають не з дзвінка, а з повідомлення: фейкова виплата, голосування, прохання від знайомого або «підтримка» в месенджері.

Фейкова підтримка

Не шукайте контакти банку через Google або випадкові чати. Пишіть у підтримку зсередини mono.

Підозріле посилання

Перевіряйте адресу. Зайві літери, дивні символи або чужий домен - привід закрити сторінку.

Прохання про гроші

Якщо знайомий просить переказати кошти в месенджері, краще передзвоніть йому окремо.

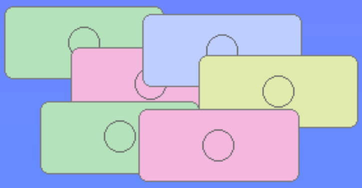
пам'ятка клієнта

Що ніколи не передавати

Жоден працівник банку не потребує ваших секретних даних, щоб «захистити» рахунок. Якщо ці дані просять - контакт треба припинити.

- ✓ CVV/CVC і повний номер картки
- ✓ PIN-код і пароль до банкінгу
- ✓ SMS-коди та push-коди підтвердження
- ✓ коди для SIM/eSIM або зміни номера
- ✓ доступ до екрана через сторонні програми
- ✓ переказ «для перевірки» чи «порятунку»

Безпечна відповідь одна: нічого не повідомляти, нічого не встановлювати і самостійно перевірити ситуацію в застосунку.



пам'ятка клієнта

Якщо ви вже відповіли шахраям

Не чекайте наступного дзвінка. Чим швидше ви обмежите доступ, тим менше шансів на втрату коштів.

План дій

- заблокуйте картку або рахунок у застосунку
- змініть PIN, пароль і доступ до фінансового номера
- видаліть підозрілі програми, якщо їх встановлювали
- перевірте історію операцій і зафіксуйте підозрілі списання
- зверніться в підтримку mono та збережіть скриншоти, номер і час контакту

Коротко

Не довіряйте терміновості, не передавайте коди, не встановлюйте програми і не переказуйте гроші за інструкцією незнайомця.